

What is claimed is:

1 1. A system for automatically protecting private video content using
2 embedded cryptographic security, comprising:

3 a recorder frame buffer dividing a substantially continuous video signal
4 representing raw video content into individual frames which each store a fixed
5 amount of data in digital form;

6 an encryption module encrypting each individual frame into encrypted
7 video content using an encryption cryptographic key and storing the encrypted
8 frames on a transportable storage medium;

9 a decryption module retrieving encrypted frames from the transportable
10 storage medium and decrypting each encrypted frame using a decryption
11 cryptographic key that is verified prior to decryption; and

12 a playback frame buffer combining the decrypted frames into a
13 substantially continuous video signal representing the raw video content in
14 reconstructed form.

1 2. A system according to Claim 1, further comprising:

2 a signature module generating a fixed-length original cryptographic hash
3 from at least one such individual frame, encrypting the original cryptographic
4 hash using an encryption cryptographic key, and storing the encrypted original
5 cryptographic hash as a digital signature on the transportable storage medium;

6 a verification module retrieving the digital signature from the
7 transportable storage medium, decrypting the encrypted original cryptographic
8 hash using a decryption cryptographic key, generating a verification fixed-length
9 cryptographic hash from at least one such individual frame, and comparing the
10 verification cryptographic hash and the original cryptographic hash.

1 3. A system according to Claim 2, further comprising:

2 an asymmetric cryptographic key pair comprising a private key
3 corresponding to the encryption cryptographic key and a public key
4 corresponding to the decryption cryptographic key.

- 1 4. A system according to Claim 1, further comprising:
2 a validation module validating the decryption cryptographic key against
3 user-provided credentials prior to decrypting the encrypted frames.
- 1 5. A system according to Claim 1, further comprising:
2 an asymmetric cryptographic key pair comprising a public key
3 corresponding to the encryption cryptographic key and a private key
4 corresponding to the decryption cryptographic key.
- 1 6. A system according to Claim 5, wherein the asymmetric
2 cryptographic key pair comprises at least one of an RSA-compatible key pair, a
3 TwoFish-compatible key pair and a Diffie-Hellman-compatible key pair.
- 1 7. A system according to Claim 1, further comprising:
2 a symmetric cryptographic key pair comprising a substantially identical
3 key corresponding to each of the encryption cryptographic key and the decryption
4 cryptographic key.
- 1 8. A system according to Claim 1, further comprising:
2 a removable storage medium storing at least one of the encryption
3 cryptographic key and the decryption cryptographic key.
- 1 9. A system according to Claim 8, further comprising:
2 a set of cryptographic instructions stored on the removable storage
3 medium and employing at least one of the encryption cryptographic key and the
4 decryption cryptographic key.
- 1 10. A method for automatically protecting private video content using
2 embedded cryptographic security, comprising:
3 dividing a substantially continuous video signal representing raw video
4 content into individual frames which each store a fixed amount of data in digital
5 form;

6 encrypting each individual frame into encrypted video content using an
7 encryption cryptographic key and storing the encrypted frames on a transportable
8 storage medium;
9 retrieving encrypted frames from the transportable storage medium and
10 decrypting each encrypted frame using a decryption cryptographic key that is
11 verified prior to decryption; and
12 combining the decrypted frames into a substantially continuous video
13 signal representing the raw video content in reconstructed form.

1 11. A method according to Claim 10, further comprising:
2 generating a fixed-length original cryptographic hash from at least one
3 such individual frame;
4 encrypting the original cryptographic hash using an encryption
5 cryptographic key and storing the encrypted original cryptographic hash as a
6 digital signature on the transportable storage medium;
7 retrieving the digital signature from the transportable storage medium and
8 decrypting the encrypted original cryptographic hash using a decryption
9 cryptographic key; and
10 generating a verification fixed-length cryptographic hash from at least one
11 such individual frame and comparing the verification cryptographic hash and the
12 original cryptographic hash.

1 12. A method according to Claim 11, further comprising:
2 providing an asymmetric cryptographic key pair comprising a private key
3 corresponding to the encryption cryptographic key and a public key
4 corresponding to the decryption cryptographic key.

1 13. A method according to Claim 10, further comprising:
2 validating the decryption cryptographic key against user-provided
3 credentials prior to decrypting the encrypted frames.

1 14. A method according to Claim 10, further comprising:

2 providing an asymmetric cryptographic key pair comprising a public key
3 corresponding to the encryption cryptographic key and a private key
4 corresponding to the decryption cryptographic key.

1 15. A method according to Claim 14, wherein the asymmetric
2 cryptographic key pair comprises at least one of an RSA-compatible key pair, a
3 TwoFish-compatible key pair and a Diffie-Hellman-compatible key pair.

1 16. A method according to Claim 10, further comprising:
2 providing a symmetric cryptographic key pair comprising a substantially
3 identical key corresponding to each of the encryption cryptographic key and the
4 decryption cryptographic key.

1 17. A method according to Claim 10, further comprising:
2 providing at least one of the encryption cryptographic key and the
3 decryption cryptographic key on a removable storage medium.

1 18. A method according to Claim 17, further comprising:
2 including a set of cryptographic instructions employing at least one of the
3 encryption cryptographic key and the decryption cryptographic key on the
4 removable storage medium.

1 19. A computer-readable storage medium holding code for performing
2 the method according to Claims 10, 11, 12, 13, 14, 15, 16, 17, or 18.

1 20. A system for encrypting private video content using embedded
2 cryptographic security, comprising:
3 a frame buffer receiving a substantially continuous video signal
4 representing raw video content and dividing the data signal into individual frames
5 which each store a fixed amount of data in digital form;
6 a processor encrypting each individual frame into encrypted video content
7 using an encryption key selected from a cryptographic key pair; and

8 a recorder storing the encrypted frames on a transportable storage medium
9 for retrieval and decryption using a decryption key selected from the
10 cryptographic key pair.

1 21. A system according to Claim 20, comprising:

2 the processor generating a fixed-length original cryptographic hash from
3 at least one such individual frame and encrypting the original cryptographic hash
4 using an encryption cryptographic key selected from the cryptographic key pair;
5 and

6 the recorder storing the encrypted original cryptographic hash as a digital
7 signature on the transportable storage medium for retrieval and verification using
8 a decryption key selected from the cryptographic key pair.

1 22. A system according to Claim 21, further comprising:

2 a private key corresponding to the encryption cryptographic key and a
3 public key corresponding to the decryption cryptographic key.

1 23. A system according to Claim 20, further comprising:

2 a public key corresponding to the encryption cryptographic key and a
3 private key corresponding to the decryption cryptographic key.

1 24. A system according to Claim 20, further comprising:

2 a substantially identical key corresponding to each of the encryption
3 cryptographic key and the decryption cryptographic key.

1 25. A system according to Claim 20, further comprising:

2 a removable storage medium storing at least one of the encryption
3 cryptographic key and the decryption cryptographic key.

1 26. A method for encrypting private video content using embedded
2 cryptographic security, comprising:

3 receiving a substantially continuous video signal representing raw video
4 content and dividing the data signal into individual frames which each store a
5 fixed amount of data in digital form;

6 encrypting each individual frame into encrypted video content using an
7 encryption key selected from a cryptographic key pair; and
8 storing the encrypted frames on a transportable storage medium for
9 retrieval and decryption using a decryption key selected from the cryptographic
10 key pair.

1 27. A method according to Claim 26, further comprising:
2 generating a fixed-length original cryptographic hash from at least one
3 such individual frame;
4 encrypting the original cryptographic hash using an encryption
5 cryptographic key selected from the cryptographic key pair; and
6 storing the encrypted original cryptographic hash as a digital signature on
7 the transportable storage medium for retrieval and verification using a decryption
8 key selected from the cryptographic key pair.

1 28. A method according to Claim 27, further comprising:
2 employing a private key corresponding to the encryption cryptographic
3 key and a public key corresponding to the decryption cryptographic key.

1 29. A method according to Claim 26, further comprising:
2 employing a public key corresponding to the encryption cryptographic key
3 and a private key corresponding to the decryption cryptographic key.

1 30. A method according to Claim 26, further comprising:
2 employing a substantially identical key corresponding to each of the
3 encryption cryptographic key and the decryption cryptographic key.

1 31. A method according to Claim 26, further comprising:
2 providing at least one of the encryption cryptographic key and the
3 decryption cryptographic key on a removable storage medium.

1 32. A computer-readable storage medium holding code for performing
2 the method according to Claims 26, 27, 28, 29, 30 or 31.

1 33. A system for decrypting private video content using embedded
2 cryptographic security, comprising:
3 a player retrieving encrypted frames from a transportable storage medium,
4 the encrypted frames storing raw video content encrypted using an encryption
5 cryptographic key selected from a cryptographic key pair;
6 a processor decrypting each encrypted frame using a decryption
7 cryptographic key selected from the cryptographic key pair; and
8 a frame buffer combining the decrypted frames into a substantially
9 continuous video signal representing the raw video content in reconstructed form.

1 34. A system according to Claim 33, comprising:
2 the player retrieving a digital signature from the transportable storage
3 medium, the digital signature containing an original cryptographic hash encrypted
4 using an encryption cryptographic key selected from the cryptographic key pair;
5 the processor decrypting the encrypted original cryptographic hash using a
6 decryption cryptographic key selected from the cryptographic key pair, generating
7 a verification fixed-length cryptographic hash from at least one individual frame
8 retrieved from the transportable storage medium, and comparing the verification
9 cryptographic hash and the original cryptographic hash.

1 35. A system according to Claim 34, further comprising:
2 a public key corresponding to the encryption cryptographic key and a
3 private key corresponding to the decryption cryptographic key.

1 36. A system according to Claim 33, further comprising:
2 a public key corresponding to the encryption cryptographic key and a
3 private key corresponding to the decryption cryptographic key.

1 37. A system according to Claim 33, further comprising:
2 a substantially identical key corresponding to each of the encryption
3 cryptographic key and the decryption cryptographic key.

1 38. A system according to Claim 33, further comprising:

2 a removable storage medium storing at least one of the encryption
3 cryptographic key and the decryption cryptographic key.

1 39. A method for decrypting private video content using embedded
2 cryptographic security, comprising:

3 retrieving encrypted frames from a transportable storage medium, the
4 encrypted frames storing raw video content encrypted using an encryption
5 cryptographic key selected from a cryptographic key pair;

6 decrypting each encrypted frame using a decryption cryptographic key
7 selected from the cryptographic key pair; and

8 combining the decrypted frames into a substantially continuous video
9 signal representing the raw video content in reconstructed form.

1 40. A method according to Claim 39, comprising:

2 retrieving a digital signature from the transportable storage medium, the
3 digital signature containing an original cryptographic hash encrypted using an
4 encryption cryptographic key selected from the cryptographic key pair;

5 decrypting the encrypted original cryptographic hash using a decryption
6 cryptographic key selected from the cryptographic key pair; and

7 generating a verification fixed-length cryptographic hash from at least one
8 individual frame retrieved from the transportable storage medium and comparing
9 the verification cryptographic hash and the original cryptographic hash.

1 41. A method according to Claim 40, further comprising:

2 employing a public key corresponding to the encryption cryptographic key
3 and a private key corresponding to the decryption cryptographic key.

1 42. A method according to Claim 39, further comprising:

2 employing a public key corresponding to the encryption cryptographic key
3 and a private key corresponding to the decryption cryptographic key.

1 43. A method according to Claim 39, further comprising:

2 employing a substantially identical key corresponding to each of the
3 encryption cryptographic key and the decryption cryptographic key.

1 44. A method according to Claim 39, further comprising:
2 providing at least one of the encryption cryptographic key and the
3 decryption cryptographic key on a removable storage medium.

1 45. A computer-readable storage medium holding code for performing
2 the method according to Claims 39, 40, 41, 42, 43 or 44.

1 46. A system for automatically authenticating private video content
2 using embedded cryptographic security, comprising:
3 a recorder frame buffer dividing a substantially continuous video signal
4 representing raw video content into individual frames which each store a fixed
5 amount of data in digital form;
6 a signature module generating a fixed-length original cryptographic hash
7 from at least one such individual frame, encrypting the original cryptographic
8 hash using an encryption cryptographic key, and storing the encrypted original
9 cryptographic hash as a digital signature on a transportable storage medium;
10 a verification module retrieving the digital signature from the
11 transportable storage medium and decrypting the encrypted original cryptographic
12 hash using a decryption cryptographic key; and
13 a player frame buffer generating a verification fixed-length cryptographic
14 hash from at least one such individual frame and comparing the verification
15 cryptographic hash and the original cryptographic hash.

1 47. A system according to Claim 46, further comprising:
2 an asymmetric cryptographic key pair comprising a private key
3 corresponding to the encryption cryptographic key and a public key
4 corresponding to the decryption cryptographic key.

1 48. A system according to Claim 47, wherein the asymmetric
2 cryptographic key pair comprises at least one of an RSA-compatible key pair, a
3 TwoFish-compatible key pair and a Diffie-Hellman-compatible key pair.

1 49. A system according to Claim 46, further comprising:
2 a removable storage medium storing at least one of the encryption
3 cryptographic key and the decryption cryptographic key.

1 50. A system according to Claim 49, further comprising:
2 a set of cryptographic instructions employing at least one of the encryption
3 cryptographic key and the decryption cryptographic key stored on the removable
4 storage medium.

1 51. A method for automatically authenticating private video content
2 using embedded cryptographic security, comprising:
3 dividing a substantially continuous video signal representing raw video
4 content into individual frames which each store a fixed amount of data in digital
5 form and generating a fixed-length original cryptographic hash from at least one
6 such individual frame;
7 encrypting the original cryptographic hash using an encryption
8 cryptographic key and storing the encrypted original cryptographic hash as a
9 digital signature on a transportable storage medium;
10 retrieving the digital signature from the transportable storage medium and
11 decrypting the encrypted original cryptographic hash using a decryption
12 cryptographic key; and
13 generating a verification fixed-length cryptographic hash from at least one
14 such individual frame and comparing the verification cryptographic hash and the
15 original cryptographic hash.

1 52. A method according to Claim 51, further comprising:

2 providing an asymmetric cryptographic key pair comprising a private key
3 corresponding to the encryption cryptographic key and a public key
4 corresponding to the decryption cryptographic key.

1 53. A method according to Claim 52, wherein the asymmetric
2 cryptographic key pair comprises at least one of an RSA-compatible key pair, a
3 TwoFish-compatible key pair and a Diffie-Hellman-compatible key pair.

1 54. A method according to Claim 51, further comprising:
2 providing at least one of the encryption cryptographic key and the
3 decryption cryptographic key on a removable storage medium.

1 55. A method according to Claim 54, further comprising:
2 including a set of cryptographic instructions employing at least one of the
3 encryption cryptographic key and the decryption cryptographic key on the
4 removable storage medium.

1 56. A computer-readable storage medium holding code for performing
2 the method according to Claims 51, 52, 54 or 55.

1 57. A system for digitally signing private video content using
2 embedded cryptographic security, comprising:
3 a frame buffer receiving a substantially continuous video signal
4 representing raw video content and dividing the data signal into individual frames
5 which each store a fixed amount of data in digital form;
6 a processor generating a fixed-length original cryptographic hash from at
7 least one such individual frame and encrypting the original cryptographic hash
8 using an encryption cryptographic key selected from a cryptographic key pair;
9 and
10 a recorder storing the encrypted original cryptographic hash as a digital
11 signature on a transportable storage medium for retrieval and verification using a
12 decryption key selected from the cryptographic key pair.

1 58. A system according to Claim 57, further comprising:

2 a private key corresponding to the encryption cryptographic key and a
3 public key corresponding to the decryption cryptographic key.

1 59. A system according to Claim 57, further comprising:
2 a removable storage medium storing at least one of the encryption
3 cryptographic key and the decryption cryptographic key.

1 60. A method for digitally signing private video content using
2 embedded cryptographic security, comprising:
3 receiving a substantially continuous video signal representing raw video
4 content and dividing the data signal into individual frames which each store a
5 fixed amount of data in digital form;
6 generating a fixed-length original cryptographic hash from at least one
7 such individual frame;
8 encrypting the original cryptographic hash using an encryption
9 cryptographic key selected from a cryptographic key pair; and
10 storing the encrypted original cryptographic hash as a digital signature on
11 a transportable storage medium for retrieval and verification using a decryption
12 key selected from the cryptographic key pair.

1 61. A method according to Claim 60, further comprising:
2 employing a private key corresponding to the encryption cryptographic
3 key and a public key corresponding to the decryption cryptographic key.

1 62. A method according to Claim 60, further comprising:
2 providing at least one of the encryption cryptographic key and the
3 decryption cryptographic key on a removable storage medium.

1 63. A computer-readable storage medium holding code for performing
2 the method according to Claims 60, 61 or 62.

1 64. A system for verifying digitally signed private video content using
2 embedded cryptographic security, comprising:

3 a player retrieving a digital signature from a transportable storage
4 medium, the digital signature containing an original cryptographic hash encrypted
5 using an encryption cryptographic key selected from a cryptographic key pair;
6 a processor decrypting the encrypted original cryptographic hash using a
7 decryption cryptographic key selected from the cryptographic key pair, generating
8 a verification fixed-length cryptographic hash from at least one individual frame
9 retrieved from the transportable storage medium, and comparing the verification
10 cryptographic hash and the original cryptographic hash.

1 65. A system according to Claim 64, further comprising:
2 a public key corresponding to the encryption cryptographic key and a
3 private key corresponding to the decryption cryptographic key.

1 66. A system according to Claim 64, further comprising:
2 a removable storage medium storing at least one of the encryption
3 cryptographic key and the decryption cryptographic key.

1 67. A method for verifying digitally signed private video content using
2 embedded cryptographic security, comprising:
3 retrieving a digital signature from a transportable storage medium, the
4 digital signature containing an original cryptographic hash encrypted using an
5 encryption cryptographic key selected from a cryptographic key pair;
6 decrypting the encrypted original cryptographic hash using a decryption
7 cryptographic key selected from the cryptographic key pair; and
8 generating a verification fixed-length cryptographic hash from at least one
9 individual frame retrieved from the transportable storage medium and comparing
10 the verification cryptographic hash and the original cryptographic hash.

1 68. A method according to Claim 67, further comprising:
2 employing a public key corresponding to the encryption cryptographic key
3 and a private key corresponding to the decryption cryptographic key.

1 69. A method according to Claim 67, further comprising:

2 providing at least one of the encryption cryptographic key and the
3 decryption cryptographic key on a removable storage medium.

1 70. A computer-readable storage medium holding code for performing
2 the method according to Claims 67, 68 or 69.

09934603-034604